EXHIBIT 22

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE GOOGLE PLAY STORE ANTITRUST LITIGATION

THIS DOCUMENT RELATES TO:

Epic Games, Inc. v. Google LLC et al., Case No. 3:20-cv-05671-JD

In re Google Play Consumer Antitrust Litigation, Case No. 3:20-cv-05761-JD

State of Utah et al. v. Google LLC et al., Case No. 3:21-cv-05227-JD

Match Group, LLC et al. v. Google LLC et al., Case No. 3:22-cv-02746-JD

Case No. 3:21-md-02981-JD

Judge: Hon. James Donato

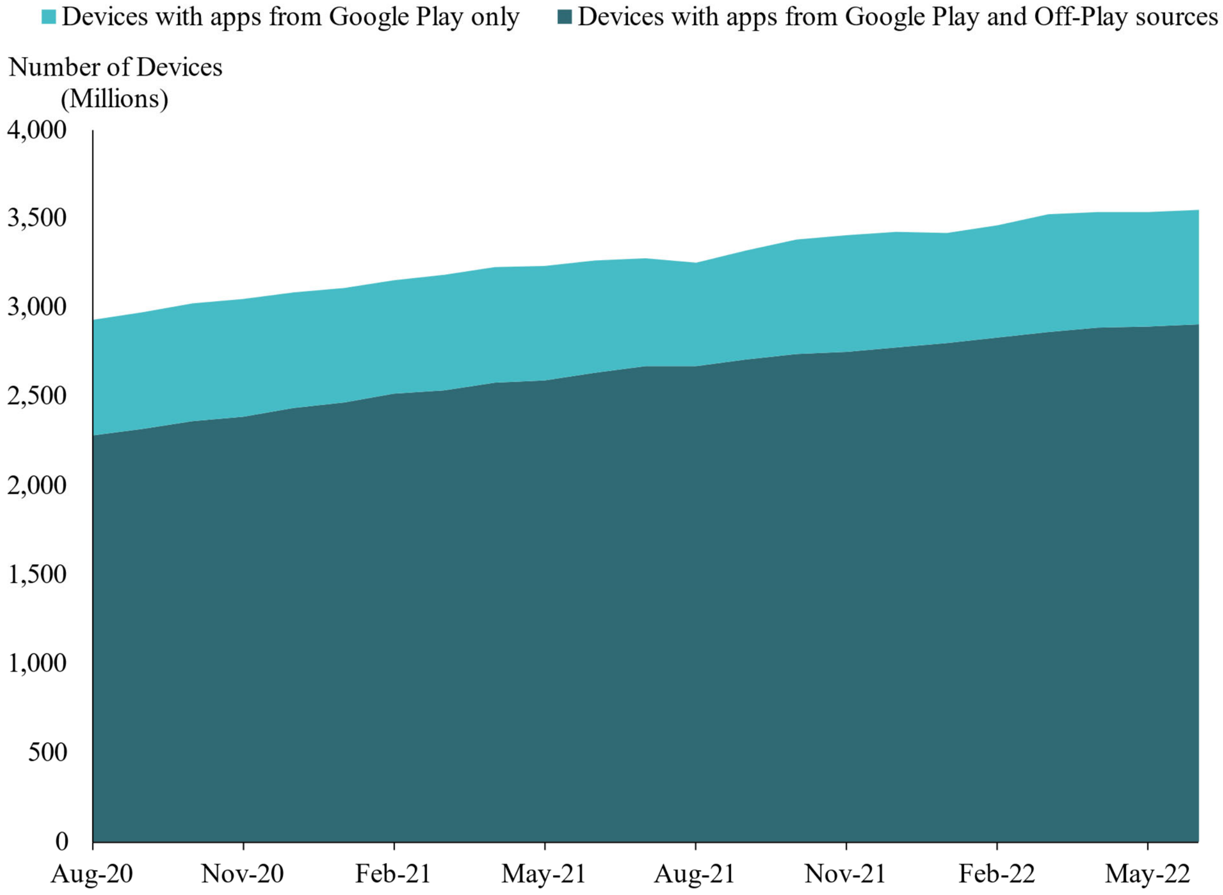
EXPERT REPORT OF ZHIYUN QIAN

NON-PARTY HIGHLY CONFIDENTIAL
OUTSIDE COUNSEL EYES ONLY

PARAGRAPHS 403-405 RESTRICTED CONFIDENTIAL - SOURCE CODE

NOVEMBER 18, 2022

Figure 5. Number of GMS Devices with Apps by Source, 2020-2022[210]



137. According to Google's data covering GMS devices globally (excluding China), from 2017 to 2020, devices that installed apps from Off-Play channels were 3.2 to 9.8 times more likely to be affected by PHAs[211] compared to devices that installed apps from Google Play only, as shown in **Figure 6** below.[212] From 2016 to 2018, the percentage of PHA installations

[210] Data are provided monthly and include GMS devices only. "Devices with apps from Google Play only" includes devices with preinstalled apps and, to the extent the user also downloaded any further apps, those were downloaded from Google Play only. It's also possible that these devices have not downloaded any apps at all (and therefore have only the preinstalled apps on them). "Devices with apps from Google Play and Off-Play sources" includes devices that have downloaded at least one app from outside of Google Play either through a user-installed app store or via sideloading. GOOG-PLAY-011354602.

[211] PHAs, or Potentially Harmful Applications, are discussed above in **Section IV**.

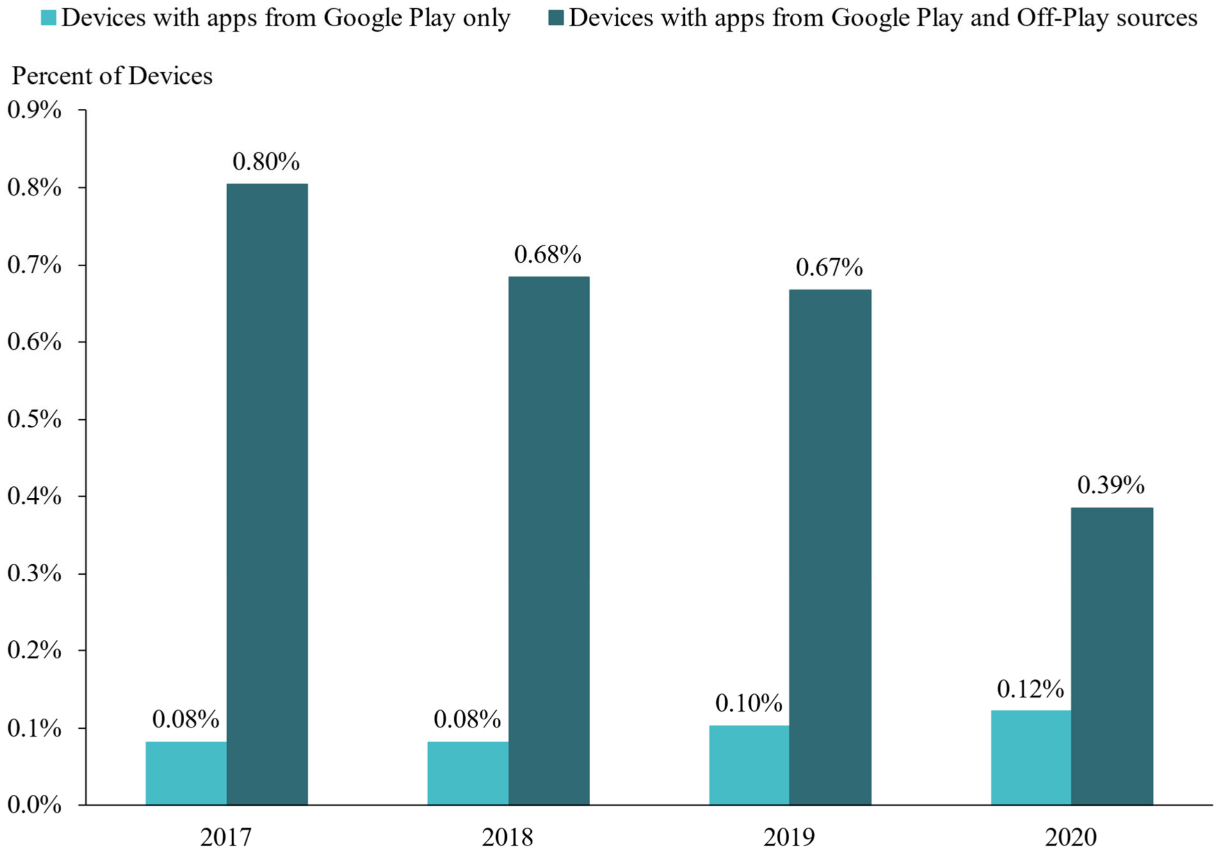
[212] These ratios were calculated by comparing the weighted averages of daily data for each respective year for devices that did and did not download apps exclusively from Google Play. (The ratios were calculated as 0.8048/0.0822 = 9.8 and 0.3851/0.1217 = 3.2. **Figure 6** shows rounded percentages). GOOG-PLAY-000379096.

was minimal for apps from Google Play in comparison to apps from Off-Play channels, as seen in **Figure 7** below.[213,214]

[213] The PHA install rate reflects the number of PHAs relative to the number of app installations across all GMS devices. Stated differently, **Figure 6**Figure 6 presents PHA data by device, whereas **Figure 7**Figure 7 reflects PHA data by installations. "Android Security & Privacy 2018 Year in Review," Google, March 2019, p. 19.

[214] The most recent available data point (June 29, 2022) suggests that the percentage of PHA installations from Google Play remains relatively unchanged at 0.05%. "Android ecosystem security," Google Transparency Report, available at https://transparencyreport.google.com/android-security/store-app-safety?hl=en. Last accessed on September 1, 2022.

Figure 6. Percentage of GMS devices with PHAs installed, 2017-2020[215,216,217]

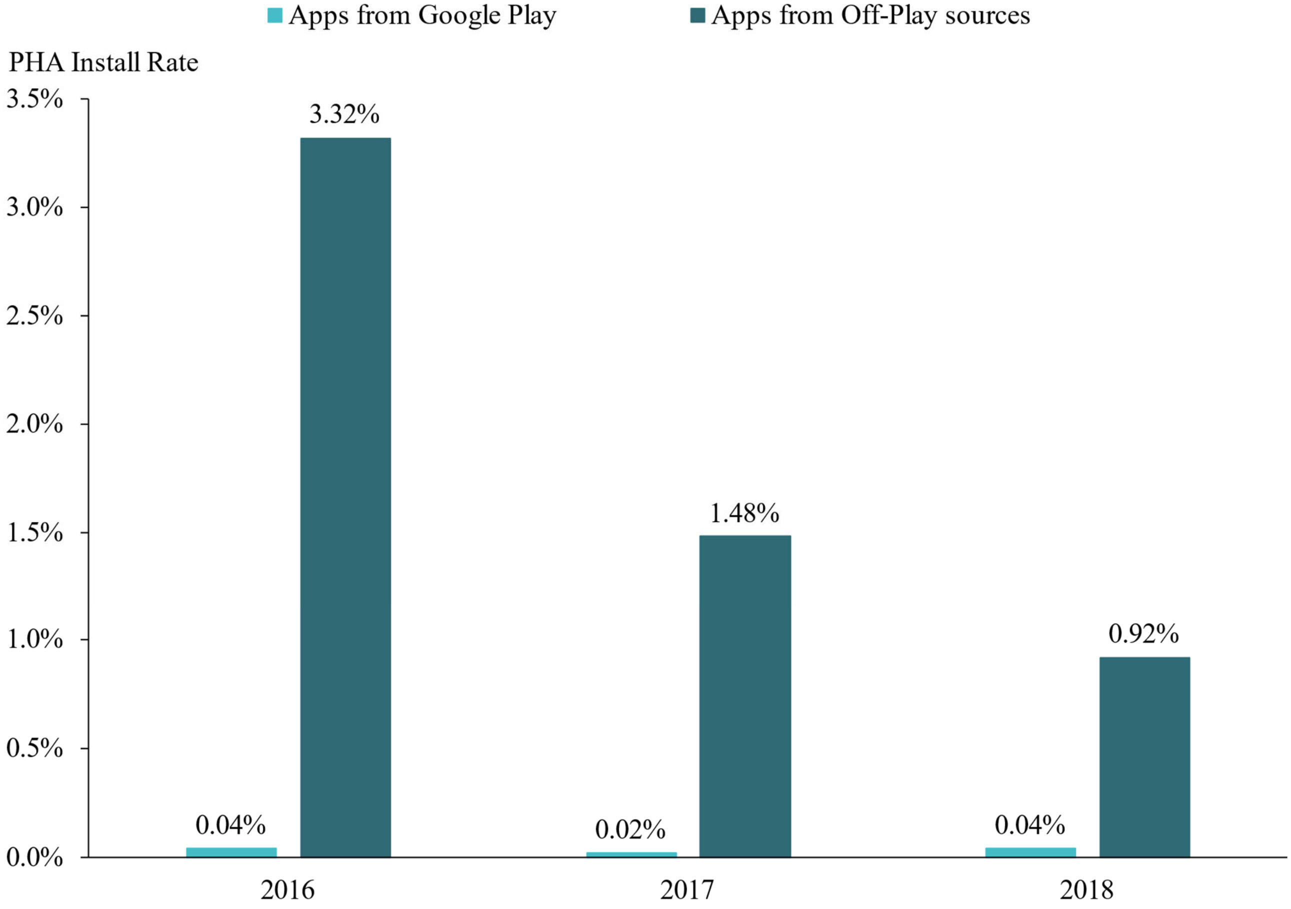


[215] GOOG-PLAY-000379096.

[216] Percentages reflect the weighted averages of daily data for devices that did and did not download apps exclusively from Google Play, for each respective year. "Devices with apps from Google Play only" includes devices with preinstalled apps and, to the extent the user also downloaded any further apps, those were downloaded from Google Play only. It is also possible that these devices have not downloaded any apps at all (and therefore have only the preinstalled apps on them). "Devices with apps from Google Play and Off-Play sources" includes devices that contain not only preinstalled apps, but also have installed at least one app outside of Google Play either through a user-installed app store or via sideloading. Definitions are supported by Google's Android Security & Privacy 2018 Year in Review Report which also presents the percentage of Android devices running Google Play Protect with PHAs installed. "Android Security & Privacy 2018 Year in Review," Google, March 2019, p. 15.

[217] The figure contains the latest data available to me. While the percentage of devices with apps from both Google Play and Off-Play sources that contain PHAs has decreased over time, the comparable percentage for devices with apps from Google Play only is still substantially lower. Additionally, I understand that this decrease is due partly to the fact that Google has updated the method by which it tracks PHAs in Off-Play sources, and partly to Google's improved processes for preventing the installation of PHAs in apps from Off-Play sources (via GPP, which launched in May 2017, as described in **Section VII**). Deposition of Sebastian Porst Day 1, 32:15-25 and Cunningham, Ed. Personal Interview. November 4, 2022.

Figure 7. Percentage of PHA installations by source, 2016-2018[218,219]



138. Google's publicly available information also notes that GMS devices with apps installed only from Google Play were significantly less likely to be affected by PHAs. For example, in 2018, the rate of PHAs in GMS devices using apps downloaded exclusively from Google Play was 0.08%, in contrast to devices using apps downloaded from Off-Play channels, which stood at 0.68%.[220] In other words, users who installed apps from outside Google Play

[218] The PHA install rate reflects the number of PHAs relative to the number of app installations across all Android devices. Stated differently, **Figure 6**Figure 6 presents PHA data by device, whereas **Figure 7**Figure 7 reflects PHA data by installations. "Android Security & Privacy 2018 Year in Review," Google, March 2019, p. 19.

[219] The figure contains the latest data available to me. While the percentage of PHA installations from apps from Off-Play sources has decreased over time, the comparable percentage from Google Play is still substantially lower. Additionally, I understand that this decrease is due partly to the fact that Google has updated the method by which it tracks PHAs in Off-Play sources, and partly to Google's improved processes for preventing the installation of PHAs in apps from Off-Play sources (via GPP, which launched in May 2017, as described in **Section VII**). Deposition of Sebastian Porst Day 1, 32:15-25.

[220] "Android Security & Privacy 2018 Year in Review," Google, March 2019, p. 15.

were 8.3 times more likely to have PHAs on their devices than those users who installed their apps exclusively from Google Play.[221]

139. The Schmidt Report criticizes Google's PHA data. In particular, the Report includes claims that: (1) there are discrepancies in measuring PHA *installations* versus PHAs *active on devices*,[222] (2) the statistics for Off-Play sources include PHAs in preinstalled apps, which is a different infection vector from sideloading,[223] and (3) some PHAs may be desired by users, such as apps used for "rooting"[224] a device to unlock certain functionalities that are otherwise difficult to access.[225]

140. None of these points refute the fact that Off-Play sources have a greater risk of malware than Google Play. Regarding Prof. Schmidt's first point, I find similar relative differences in risk between Google Play and Off-Play sources when using data on either PHA installations or PHAs on devices.[226] There are also other empirical studies by independent academics, not using Google's data, that indicate that the PHA installation rate is significantly lower when users only use Google Play.[227] Regarding Prof. Schmidt's second point, the fact that preinstalled apps have security risks (which they do, as I discuss further in **Section V.C.2** below) does not diminish the security risks from sideloading, as the PHA installation rate captures. Regarding Prof. Schmidt's third point, certain "user-wanted" apps are not classified

[221] Using the aforementioned statistics on PHA rates among apps installed via Google Play and Off-Play channels, respectively (0.6847/0.0821 = 8.3. **Figure 6** shows rounded percentages).

[222] Schmidt Report, ¶¶ 129-130.

[223] Schmidt Report, ¶ 132.

[224] Rooted devices are those which have been "jailbroken to install unapproved apps, update OS, delete unwanted apps, underclock or overclock the processor, replace firmware and customize anything else." Cole, Arthur, "Things You Need to Know before Rooting Your Android Device," Clever Files, August 11, 2020, available at https://www.cleverfiles.com/howto/what-is-rooted-device.html. Last accessed on March 10, 2022.

[225] Schmidt Report, ¶ 131.

[226] According to the Schmidt Report, Google undercounts the number of devices with PHAs from the "Google Play Only" category because Google excluded PHAs from "top partner developers" from the figure. However, I have not seen any evidence that the potential undercounting of devices applies only to devices that exclusively use Google Play, and therefore assume that Off-Play PHA numbers are subject to the same bias. Further, **Figure 7**Figure 7 features a different variable and data source (PHA installations) than the one criticized by the Schmidt Report, and suggests a consistent relative risk of "Google Play Only" and "Outside of Google Play" PHA rates. Schmidt Report, ¶ 129.

[227] This is particularly true of non-Google app stores, and I discuss several studies in **Section V.C.3** below.

by Google as a PHA even if their use entails some risk.[228]Rooting remains a potentially harmful capability that may cause irreparable harm to a device if performed incorrectly and that generally renders it less secure even when used as intended.[229,230] In accordance with the principle of secure defaults, it is therefore appropriate to warn users before they download and install apps with rooting capabilities.

141. Using the MUwS metric instead of PHAs yields similar differences in the relative rates between devices with apps exclusively from Google Play versus those that also download apps from Off-Play sources.[231] From 2019 to 2021, devices that installed apps from Off-Play channels were 1.5 to 2.7 times more likely to be affected by unwanted software than devices that installed apps from Google Play only.[232]

142. Overall, apps from Off-Play channels have, in the aggregate, a higher likelihood of being malware than apps from Google Play. In the following three subsections, I discuss in more detail security risks related to preinstalled apps, apps from non-Google app stores, and sideloaded apps.

V.C.2. Preinstalled Apps

143. Data from Google for 2018, which the Schmidt Report also cites,[233] shows that preinstalled apps ranked among the most widely spread malware threats in several of the countries with the largest number of GMS devices worldwide.[234] Preinstalled apps often run

[228] "Potentially Harmful Applications (PHAs)," Google Developers, November 12, 2019, available at https://developers.google.com/android/play-protect/potentially-harmful-applications. Last accessed on June 14, 2022.

[229] "The risks of rooting your Android phone," Norton, September 21, 2022, available at https://us.norton.com/blog/mobile/android-rooting-risks. Last accessed on October 24, 2022.

[230] Snyder, Joel, "What are the security risks of rooting your smartphone?," Samsung Insights, July 28, 2022, available at https://insights.samsung.com/2022/07/28/what-are-the-security-risks-of-rooting-your-smartphone-4/. Last accessed on November 2, 2022.

[231] I discuss MUwS in **Section IV**.

[232] These ratios were calculated by comparing annual estimates of the percentage of MUwS-affected devices, each calculated as weighted averages using quarterly data from 2019-04-01 to 2021-01-01, for devices with apps installed from "Devices with apps from Google Play only" and "Devices with apps from Google Play and Off-Play sources", respectively (53.09/35.4 = 1.5 and 36.5/13.68 = 2.7). GOOG-PLAY-000379096.

[233] Schmidt Report, ¶ 133.

[234] For instance, preinstalled apps were four of the ten most widely circulated malware threats in both Brazil and Indonesia during 2018. GOOG-PLAY-000057802-832 at 817-818.

Zhiyun Qian, Ph.D.

Date: November 18, 2022